PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-191079
(43)Date of publication of application : 13.07.1999

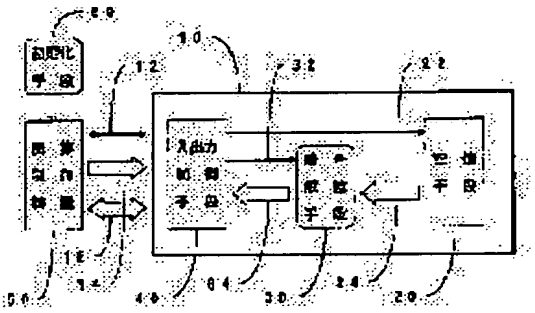
(51)Int.Cl. G06F 12/14
G11C 17/00
H01L 27/10

(21)Application number : 09-366267
(22)Date of filing : 25.12.1997

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : OSUMI YUJI

(54) SEMICONDUCTOR INTEGRATED CIRCUIT

(57)Abstract:
PROBLEM TO BE SOLVED: To secure the secrecy property of data stored in a ROM more safely by providing a data outputting part of a storing means with a decoding means, making the decoding means decode data that is enciphered and stored and outputting it.
SOLUTION: As for data that is stored in a storing means 20, data which preliminarily undergoes a certain specific kind of enciphering is stored. An input-output control means 40 is controlled by an operation controller 50 which is connected to the outside of the semiconductor integrated circuit 10 and outputs data stored in the means 20 to the outside of the circuit 10 based on a control signal that is outputted by the controller 50. A decoding means 30 is located between the means 20 and 40, uses a decoding key code that is transferred from the controller 50, has a decoding key code inputting means which decodes data of the means 20, decodes storage data (i.e. encoded data) which is outputted from the means 20 and after that transfers the decoded storage data to the means 40.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－191079

(43)公開日　平成11年(1999)７月13日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ１１Ｃ　17/00		Ｇ１１Ｃ　17/00	
Ｈ０１Ｌ　27/10		Ｈ０１Ｌ　27/10	

審査請求　未請求　請求項の数３　ＦＤ　（全６頁）

(21)出願番号　特願平9－366267

(22)出願日　平成９年(1997)12月25日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　大住　勇治
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

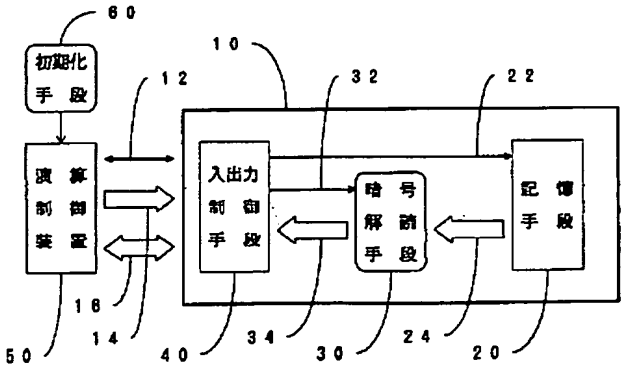
(74)代理人　弁理士　金山　聡

(54)【発明の名称】　半導体集積回路

(57)【要約】

【課題】　ＲＯＭに記憶してあるデータの機密性を確保する半導体集積回路を得る。

【解決手段】　あらかじめ、データが書き込まれた記憶手段を備えた集積回路装置において、前記記憶手段には暗号化されたデータが書き込まれており、記憶手段のデータ出力部に暗号解読手段を備え、暗号化されたデータを前記暗号解読手段で復号化して出力される半導体集積回路である。また、前記暗号解読手段は、外部から入力される暗号解読用の復号化鍵コードを用いて、記憶手段のデータを復号する復号化コード入力手段を備えている半導体集積回路である。さらに、暗号解読手段は、ＤＥＳに代表される秘密鍵方式である半導体集積回路である。



1

【特許請求の範囲】

【請求項１】　あらかじめ、データが書き込まれた記憶手段を備えた集積回路装置において、前記記憶手段には暗号化されたデータが書き込まれており、記憶手段のデータ出力部に暗号解読手段を備え、暗号化されて記憶されたデータを前記暗号解読手段で復号して出力する機能を備えたことを特徴とする半導体集積回路。

【請求項２】　請求項１に記載の半導体集積回路において、暗号解読手段は、外部から入力される暗号解読用の復号化鍵コードを用いて、記憶手段のデータを復号する復号化鍵コード入力手段を備えていることを特徴とする半導体集積回路。

【請求項３】　請求項１または請求項２の半導体集積回路において、暗号解読手段は、ＤＥＳに代表される秘密鍵方式であることを特徴とする半導体集積回路。

【請求項４】

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】半導体集積回路、特にＲＯＭ(Read Only Memory)に記憶されているプログラム、またはデータを、外部から解析できないようにするための暗号処理回路を内蔵した半導体集積回路に関するものである。

【０００２】

【従来の技術】一般にマイクロプロセッサなどのデータ処理装置には、各種プログラムやデータなどを書き込んだＲＯＭが備えられている。こうしたプログラムやデータは、処理装置の重要な機能を担うとともに、高度なノウハウを含むことが多く、従ってマイクロプロセッサなどに組み込んだあとは、容易に外部から解読できないようにする要求がある。例えば、ＲＯＭの外部端子を信号観測装置などを用いて観測したり、また、場合によっては半導体集積回路の回路パターンを分析して、ＲＯＭに記憶してあるデータの内容を解読するなどの試みがなされることがあり、これらの試みに対するデータ保護のために、種々の提案がなされている。

【０００３】ＲＯＭに記憶してあるデータの外部からの観測を困難にする方法としては、例えば、主メモリとは別に暗号コードを記憶するメモリを設け、入力コードと暗号コードが一致したときのみ主メモリのデータの読み出しが可能になる装置（第１の従来例：特開平３－２７８１５１）が提案されている。また、ＲＯＭに記憶してあるデータを外部に出力するとき暗号化して出力し、出力された暗号化データを解読する装置を別に設ける方法（第２の従来例：特開平２－３００８３４）がある。さらに、ＥＥＰＲＯＭ(Electrically Erasable and Programmable Read Only Memory）に書き込むデータを暗号化する装置を、ＲＯＭのデータ入力部に設け、また、ＲＯＭのデータ出力部に、暗号復号器を設けておき、さらに、ＲＯＭに書き込むデータの暗号化、およびＲＯＭから読み出すデータの復号化に使用する暗号コードのラッチ回路を設け、暗号化されたＲＯＭデータを外部に出力するとき、先ず、暗号コードを入力し、正しい暗号コードが入力されたときのみ、外部に出力されるＲＯＭデータが正しいデータになるようにした半導体装置（第３の従来例：特開平１－１６２９５７）などが提案されている。

2

【０００４】

【発明が解決しようとする課題】前述した目的に使用されるＲＯＭの種類としては、ＥＰＲＯＭ、ＥＥＰＲＯＭ、フラッシュＲＯＭなど各種のＲＯＭを使用することができるが、大容量で信頼性が高く、かつ低価格であるマスクＲＯＭが使用されることが多い。しかし、マスクＲＯＭは、集積回路の配線パターンによってデータを記憶する構造になっているため、配線パターンの解析により、ＲＯＭに記憶してあるデータが解析され、集積回路を不正に複製されるおそれがあり、プログラムやデータの機密性を保つことが困難であった。このように、マスクＲＯＭは基本的で重要なプログラムやデータを格納することが多いにもかかわらず、集積回路の配線パターンが規則的な構造のため解読されやすかった。

【０００５】すなわち、第１の従来例に示した集積回路装置では、集積回路を分解して回路パターンを解析することによってＲＯＭに記憶してあるデータを簡単に解読できる。また、第２の従来例では、第１の従来例と同様に集積回路を分解して回路パターンを解析することによってＲＯＭに記憶してあるデータを簡単に解読でき、また、ＲＯＭに記憶してあるデータを外部の装置に出力するときに暗号化しているので、暗号化のための装置を集積回路に組み込む必要があり、さらに、外部の装置には暗号化したデータを復号化する装置も必要になるので、装置全体のコストが高くなる欠点がある。また、第３の従来例では、ＲＯＭに記憶するデータの暗号化装置と、記憶されたデータの復号化装置を半導体集積回路上に組み込むので、集積回路の製造コストが高くなる欠点がある。

【０００６】本発明は、上記従来装置における課題を解決するとともに、より安全にＲＯＭに記憶するデータの機密性を確保することを目的としてなさたものである。以下に本課題の解決手段について説明する。

【０００７】

【課題を解決するための手段】すなわち、本発明は、請求項１に示すように、あらかじめ、データが書き込まれた記憶手段を備えた集積回路装置において、前記記憶手段には暗号化されたデータが書き込まれており、記憶手段のデータ出力部に暗号解読手段を備え、暗号化されて記憶されたデータを、前記暗号解読手段で復号化して出力する半導体集積回路である。また、本発明は、請求項２に示すように、請求項１の発明に加えて、暗号解読手段は、外部から入力される暗号解読用の復号化鍵コード

を用いて、記憶手段のデータを復号する復号化鍵コード入力手段を備えている半導体集積回路である。さらに、本発明は、請求項３に示すように、請求項１または請求項２の発明に加えて、暗号解読手段は、ＤＥＳに代表される秘密鍵方式である半導体集積回路である。

【０００８】

【発明の実施の形態】次に、本発明の実施の形態について、実施例の図面を用いて詳細に説明する。なお、図１は、本発明の半導体集積回路の概略構成図である。また、図２、図３は、本発明の半導体集積回路に組み込まれる暗号解読手段の一例を示すブロック図である。

【０００９】（構成）先ず、本発明の半導体集積回路について、その構成について説明する。図１は本発明の半導体集積回路の概略構成図である。図において、１０は半導体集積回路である。半導体集積回路１０は、プログラムやデータを記憶するための記憶手段２０を内蔵している。前記記憶手段２０に記憶させるデータは、あらかじめ、ある特定の種類の暗号化を施したデータを記憶させるものとする。また、半導体集積回路１０は、前記記憶手段２０のデータを外部に出力するための、入出力制御手段４０を備えている。前記入出力制御手段４０は、半導体集積回路１０の外部に接続された演算制御装置５０によって制御され、演算制御装置５０が出力する制御信号に基づいて、記憶手段２０に記憶されているデータを、半導体集積回路１０の外部に出力する。さらに、本発明の半導体集積回路１０は、記憶手段２０と入出力制御手段４０との間に、前記記憶手段２０から出力される記憶データ（すなわち暗号化されたデータ）を解読したのち、前記入出力制御手段４０へ解読され復号化された記憶データを転送するための暗号解読手段３０を備えている。

【００１０】前記記憶手段２０は、例えば、マスクＲＯＭで構成する。本発明では、前記マスクＲＯＭに記憶させるデータを、例えば、ＤＥＳ(Data Encryption Standard)と呼ばれる米国商務省が定めた暗号標準方式によって暗号化したうえで、前記暗号化データをマスクＲＯＭの記憶データとする。マスクＲＯＭに記憶するデータを暗号化する場合、例えば、マスクＲＯＭのデータ焼き付け用フォトマスクを設計するための回路設計装置上で、マスクＲＯＭ用の記憶データを暗号化処理したうえで、前記暗号化されたデータに基づいてフォトマスクを作製し、このマスクを用いて半導体集積回路を製作することによって、集積回路のマスクＲＯＭ部に暗号化データを組み込むことができる。なお、回路設計装置上で、マスクＲＯＭに記憶させるデータを暗号化するために、あらかじめ、暗号化コードである鍵コードを決定しておく必要がある。このＤＥＳ暗号方式の鍵コードは、通常６４ビットのランダムな２進数が用いられる。

【００１１】半導体集積回路１０に組み込む暗号解読手段３０は、例えば、図３に示すような、暗号解読回路が用いられる。図３の暗号解読回路は、前記ＤＥＳ暗号化に用いた６４ビットの鍵コードＫを利用して、マスクＲＯＭで構成された記憶手段２０から出力される６４ビットの暗号化データＣを復号解読し、解読データ６４ビットＭを得るものであり、図中、破線で示す部分は、同一回路が繰り返し配設され、全体で１６段の復号化回路が構成されている。

【００１２】図において、ＩＰは暗号化データＣの初期転置回路を示し、IP^{-1}は復号された暗号化データから解読データＭを得るための逆初期転置回路を示す。また、図中において、＋符号は、排他的論理和演算回路を示し、また、ｆは、６４ビットの鍵コードＫから生成される４８ビット構成の１６種類の鍵系列コードＫ１６～Ｋ１と、Ｌ１６～Ｌ１で示される暗号化データの復号過程で生成される復号化データの上位３２ビットとの非線形演算回路を示す。なお、参考までに、前記非線形演算回路ｆの回路例を図２に示す。また、図３に示す、ＰＣ１、ＰＣ２、およびＲＳ１５～ＲＳ１は、６４ビットの鍵コードＫから、Ｋ１６～Ｋ１で示される１６種類の鍵系列コードＫｎを生成するための、転置回路および右巡回シフト回路を示す。

【００１３】（作用動作）次に、本発明の半導体集積回路１０の作用動作について説明する。図１に示すように、半導体集積回路１０は、制御バス１２、アドレスバス１４、データバス１６を介して接続された演算制御装置５０の指令によって動作する。この演算制御装置５０は、例えば、マイクロプロセッサユニットで構成され、当該マイクロプロセッサユニットの動作プログラム、または、マイクロプロセッサユニットが動作するために必要な各種データが、本発明の半導体集積回路１０に格納されている。但し、半導体集積回路１０の記憶手段２０に格納されているプログラムやデータは、前述したように、暗号化されたコードであり、そのまま、演算制御装置５０によって読み出されても、演算制御装置５０は正常に動作することはできない。本発明の半導体集積回路１０を用いて、演算制御装置５０を正常に動作させるためには、前記記憶手段２０に格納されている暗号化データを、暗号解読手段３０を介して、解読データに変換し、それを演算制御装置５０に転送する必要がある。

【００１４】次に、本発明の半導体集積回路１０を動作させる方法について説明する。図１に示すように、演算制御装置５０には、半導体集積回路１０の動作を初期化するための初期化手段６０が接続されており、この初期化手段６０は、図示していないが、例えば、ＲＡＭ、および固定磁気ディスク等の外部記憶装置で構成する。

【００１５】この構成において、演算制御装置５０は、まず最初に、前記初期化手段６０の固定磁気ディスクに記憶されたプログラムを、ＲＡＭにロードすることによって動作を開始する。前記固定磁気ディスクには、本発明の半導体集積回路１０に含まれる暗号解読手段３０の

動作に必要な、暗号解読用の復号化鍵コード６４ビットが記憶されており、先ず、演算制御装置５０が、この復号化鍵コードをＲＡＭにロードし、次いで、前記鍵コードをＲＡＭから読み出し、半導体集積回路１０に転送する。半導体集積回路１０は、入出力制御手段４０を備えており、演算制御装置５０から転送された復号化鍵コードを受け取り、これを、制御バス３２を介して暗号解読手段３０の図示しない復号化鍵コードレジスタに格納する。復号化鍵コードを受け取った暗号解読手段３０は、次に、図３に示した暗号解読回路によって、前記復号化鍵コードに基づいて、暗号化データＣの復号に必要な、Ｋ１６～Ｋ１の１６種類の鍵系列コードを生成する。以上の動作によって、半導体集積回路１０の初期化が完了し、演算制御装置５０の動作は、初期化手段６０に記憶されたプログラム動作から、半導体集積回路１０に記憶されたプログラム動作に切り替わる。

【００１６】次に、半導体集積回路１０によるプログラム動作について説明する。半導体集積回路１０による演算制御装置５０の動作は、以下の順序で進行する。先ず、演算制御装置５０は、図示しないプログラムカウンタの設定値に基づいて、次にアクセスすべきアドレス信号を、アドレスバス１４および制御バス１２を介して、半導体集積回路１０に送る。半導体集積回路１０の入出力制御手段４０は、前記アドレス信号に基づいて、制御線２２を介して記憶手段２０の所定アドレスを選択する。記憶手段２０は選択されたアドレスの暗号化データ６４ビットをデータバス２４を介して暗号解読手段３０に送る。暗号解読手段３０は、記憶手段２０から送られた暗号化データを、図３に示す暗号解読回路の暗号化データレジスタに取り込む。

【００１７】暗号解読回路に取り込まれた暗号化データ６４ビットは、初期転置回路ＩＰにてビット転置された後、２つの３２ビットデータＲ１６、Ｌ１６に分割される。次いで、前記３２ビットデータＬ１６は、図２に示す非線形演算回路ｆに入力され、先ず、拡大転置回路Ｅで４８ビットに変換された後、排他的論理和演算回路＋に入力され、４８ビットの鍵系列コードＫ１６との排他的論理和を得る。得られた４８ビットの排他的論理和は、次いで、Ｓ１～Ｓ８の選択換字回路に入力され、３２ビットの換字データに変換された後、転置回路Ｐにてビット転置される。この３２ビットの復号化データは、図３に示す排他的論理和回路＋に入力され、前記３２ビットデータＲ１６との排他的論理和を得、次段の復号化回路の入力データＬ１５になる。また、前記３２ビットデータＬ１６は、そのまま次段の復号化回路の入力データＲ１５となる。

【００１８】上記手順で、非線形演算回路ｆ、および排他的論理和回路＋からなる１６段の復号化回路を経て、Ｋ１６～Ｋ１の１６種類の鍵系列コードにて順次復号されて得た２つの３２ビットデータＲ０、Ｌ０は、最後に、逆初期転置回路IP^{-1}にて、ビット転置されて６４ビットの解読データＭとなる。この暗号解読手段３０で得られた６４ビットの解読データＭは、図１に示すデータバス３４を介して入出力制御手段４０に転送され、前記入出力制御手段４０によって、データバス１６を介して演算制御装置５０へ向けて送り出す。演算制御装置５０は、半導体集積回路１０から送り出された解読データＭを取り込み、プログラムを実行する。

【００１９】このようにして、演算制御装置５０は、図示しないプログラムカウンタを更新しながら、半導体集積回路１０に対してアドレス信号を送り出し、前記アドレス信号に対応する暗号解読データを半導体集積回路１０から得ることによって、順次プログラムを実行することができる。また必要に応じて、プログラムを実行する上で必要なデータを、半導体集積回路１０から得ることができる。

【００２０】上述の如く、本発明の半導体集積回路では、あらかじめプログラムやデータを暗号化して記憶手段２０に格納しておき、外部から、前記暗号化して記憶されたデータを解読するための復号化鍵コードを半導体集積回路へ入力することによって、半導体集積回路に内蔵している暗号解読手段３０が、前記記憶手段の暗号化データを復号し、解読データを半導体装置の外部に出力することができる。従って、もし何らかの方法で、半導体集積回路の記憶手段２０に記憶してあるデータが判明したとしても、そのデータは暗号化されているので、意味不明なデータであり、演算制御装置のプログラム動作を特定することはできない。

【００２１】（他の実施例）次に、本発明の他の実施例について説明する。上述した実施例では、半導体集積回路の暗号解読手段３０を初期化するための復号化鍵コードを、固定磁気ディスク装置に記憶しておき、ＲＡＭおよび演算制御装置を介して、本発明の半導体集積回路に入力するように構成したが、初期化手段をＲＯＭで構成してもよい。その場合は、より高速な初期化が行えることになる。また、逆に、初期化手段にキーボードなどのデータ入力手段を接続し、暗号解読用の復号化鍵コードを手で入力するように構成することもできる。その場合は、復号化鍵コードの内容を知らない人が、本発明の半導体集積回路を組み込んだ装置を使用できないようにすることが可能になる。

【００２２】また、上述の実施例では、半導体集積回路から出力される解読データが６４ビット単位となっているが、解読データを３２ビット単位、１６ビット単位、もしくは８ビット単位で出力できるように、記憶手段２０の暗号化データ読み出しアドレス制御機能、および、入出力制御手段４０からの解読データ出力制御機能を、入出力制御手段４０に設けることにより、解読データの出力ビット単位を制御するように構成してもよい。このように構成すれば、本発明の半導体集積回路を、データ

バス幅の異なる各種の演算制御装置へ接続することが可能になり、利用範囲がより広範になる。

【００２３】

【発明の効果】以上、詳細に説明した如く本発明の半導体集積回路は、請求項１に示すように、あらかじめ、データが書き込まれた記憶手段を備えた集積回路装置において、前記記憶手段には暗号化されたデータが書き込まれており、記憶手段のデータ出力部に暗号解読手段を備え、暗号化されて記憶されたデータを前記暗号解読手段で復号して出力する機能を備えたので、記憶手段に書き込まれた暗号化データを解読するのが極めて困難であり、かつ、外部に暗号解読手段を設けることなく、通常のマイクロプロセッサなどに接続して簡便に使用することができる。

【００２４】また、本発明の半導体集積回路は、請求項２に示すように、請求項１の発明に加えて、暗号解読手段は、外部から入力される暗号解読用の復号化鍵コードを用いて記憶手段のデータを復号する復号化鍵コード入力手段を備えているので、多種類の復号化鍵コードに対応できる汎用性の高い半導体集積回路を構成することができる。

【００２５】さらに、本発明の半導体集積回路は、請求項３に示すように、請求項１または請求項２の半導体集積回路において、暗号解読手段は、ＤＥＳに代表される秘密鍵方式であるので、暗号化強度が強く、暗号化データを解読するのは困難を極め、機密性が高い。

【図面の簡単な説明】

【図１】　本発明の半導体集積回路の概略構成図である。

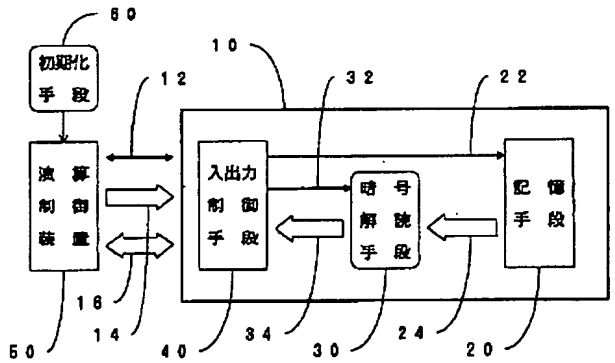
【図２】　暗号解読手段の一部を詳細に示すブロック図である。

【図３】　暗号解読手段の一例を示す回路ブロック図である。

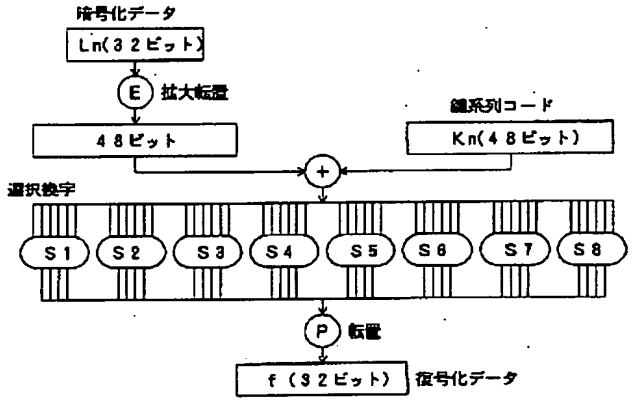
【符号の説明】

１０　半導体集積回路
２０　記憶手段
３０　暗号解読手段
４０　入出力制御手段
５０　演算制御装置
６０　初期化手段

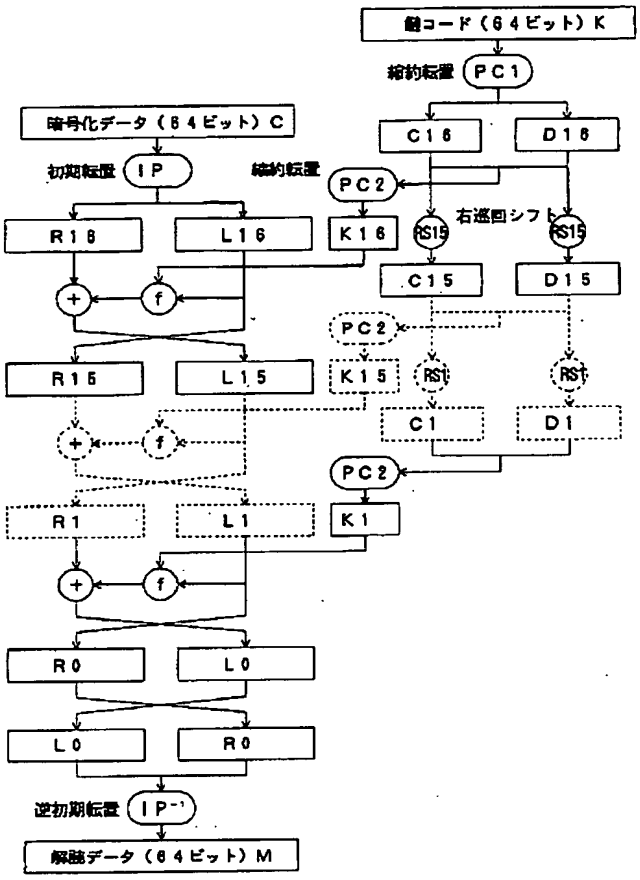
【図１】



【図２】



【図３】


鍵コード（６４ビット）K
縮約転置
PC1
暗号化データ（６４ビット）C
C16
D16
初期転置
IP
縮約転置
PC2
R16
L16
K16
RS15
右巡回シフト
RS15
C15
D15
PC2
R15
L15
K15
RS1
RS1
C1
D1
PC2
R1
L1
K1
R0
L0
L0
R0
逆初期転置
IP⁻¹
解読データ（６４ビット）M